

# Cryptography

## Past, Present and Future

Imad Fakhri Taha Al Shaikhli

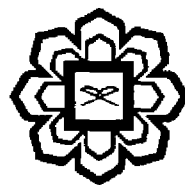


IIUM PRESS

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

# **Cryptography: Past, Present and Future**

**Imad Fakhri Taha Al Shaikhli**



IIUM Press

Published by:  
IIUM Press  
International Islamic University Malaysia

First Edition, 2011

©IIUM Press, IIUM

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without any prior written permission of the publisher.

Perpustakaan Negara Malaysia

Cataloguing-in-Publication Data

Imad Fakhri Taha Al-Shaikhli  
Cryptography: Past, Present and Future  
Imad Fakhri Taha Al-Shaikhli

ISBN: 978-967-418-091-1

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM  
(Malaysian Scholarly Publishing Council)

Printed by :  
**IIUM PRINTING SDN. BHD.**  
No. 1, Jalan Industri Batu Caves 1/3  
Taman Perindustrian Batu Caves  
Batu Caves Centre Point  
68100 Batu Caves  
Selangor Darul Ehsan

# TABLE OF CONTENTS

Dedication	I
Preface	Vii
Acknowledgement	Viii
<b>PART I Classical Cryptography</b>	<b>1</b>
<b>Chapter One Introduction</b>	<b>3-9</b>
- Imad Fakhri Taha Al Shaikhli	
- Rusydi Hasan	
- Nurhidayah Binti Abdulrashid	
- Faizurimawaty Bt Padzilah	
- Nabilah Bt Abd Rahman	
<b>Chapter Two Monoalphabetic Substitution Cipher</b>	<b>11-16</b>
- Imad Fakhri Taha Al Shaikhli	
- Rusydi Hasan	
- Nurhidayah Binti Abdulrashid	
- Faizurimawaty Bt Padzilah	
- Nabilah Bt Abd Rahman	
<b>Chapter Three Polyalphabetic Substitution Cipher</b>	<b>17-23</b>
- Imad Fakhri Taha Al Shaikhli	
- Rusydi Hasan	
- Nurhidayah Binti Abdulrashid	
- Faizurimawaty Bt Padzilah	
- Nabilah Bt Abd Rahman	
<b>Chapter Four Machine-Based Cryptography</b>	<b>25-30</b>
- Rusydi Hasan	
- Imad Fakhri Taha Al Shaikhli	
- Nurhidayah Binti Abdulrashid	
- Faizurimawaty Bt Padzilah	
- Nabilah Bt Abd Rahman	
<b>PART II Modern Symmetric-Key Cryptography</b>	<b>31</b>
<b>Chapter Five Block and Stream Cipher</b>	<b>33-38</b>
- Sufyan Salim Mahmood Al Dabbagh	
- Imad Fakhri Taha Al Shaikhli	
- Muhammad Fadil Lubis	
- Usman bin Mohd Azhar	
- Nopan Ziro Ando	
<b>Chapter Six Data Encryption Standard (DES)</b>	<b>39-46</b>
- Imad Fakhri Taha Al Shaikhli	

<ul style="list-style-type: none"> <li>- Sufyan Salim Mahmood Al Dabbagh</li> <li>- Muhammad Fadil Lubis</li> <li>- Usman bin Mohd Azhar</li> <li>- Nopan Ziro Ando</li> </ul>	
<b>Chapter Seven Advanced Encryption Standard(Rijndael)</b>	<b>47-52</b>
<ul style="list-style-type: none"> <li>- Sufyan Salim Mahmood Al Dabbagh</li> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Muhammad Fadil Lubis</li> <li>- Usman bin Mohd Azhar</li> <li>- Nopan Ziro Ando</li> </ul>	
<b>Chapter Eight Trivium and Rabbit Stream Cipher</b>	<b>53-61</b>
<ul style="list-style-type: none"> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Sufyan Salim Mahmood Al Dabbagh</li> <li>- Muhammad Fadil Lubis</li> <li>- Usman bin Mohd Azhar</li> <li>- Nopan Ziro Ando</li> </ul>	
<b>PART III Hash Functions</b>	<b>63</b>
<b>Chapter Nine Introduction</b>	<b>65-72</b>
<ul style="list-style-type: none"> <li>- Khanssaa Munthir Abdulmajed</li> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Sufyan Salim Mahmood Al Dabbagh</li> <li>- Ahmad Faridi Abdul Matin</li> <li>- Sibomana Hilali Hussein</li> </ul>	
<b>Chapter Ten Message Digest (MDX) Family</b>	<b>73-80</b>
<ul style="list-style-type: none"> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Sufyan Salim Mahmood Al Dabbagh</li> <li>- Khanssaa Munthir Abdulmajed</li> <li>- Ahmad Faridi Abdul Matin</li> <li>- Sibomana Hilali Hussein</li> </ul>	
<b>Chapter Eleven SHA family hash function</b>	<b>81-87</b>
<ul style="list-style-type: none"> <li>- Khanssaa Munthir Abdulmajed</li> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Sufyan Salim Mahmood Al Dabbagh</li> <li>- Ahmad Faridi Abdul Matin</li> <li>- Sibomana Hilali Hussein</li> </ul>	
<b>Chapter Twelve RIPEMD and Chameleon Hash Function</b>	<b>89-96</b>
<ul style="list-style-type: none"> <li>- Sufyan Salim Mahmood Al Dabbagh</li> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Khanssaa Munthir Abdulmajed</li> <li>- Ahmad Faridi Abdul Matin</li> </ul>	

- Sibomana Hilali Hussein

<b>PARTIV Public Key &amp; Digital Signature Schemes</b>	<b>97</b>
<b>Chapter Thirteen Rivest-Shamir-Adleman (RSA)</b>	<b>99-105</b>
<ul style="list-style-type: none"> <li>- Iqram Mohammed Hayek</li> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Sufyan Salim Mahmood Al Dabbagh</li> <li>- Kusai Abu Hilal</li> </ul>	
<b>Chapter Fourteen Cryptanalysis of RSA</b>	<b>107-112</b>
<ul style="list-style-type: none"> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Sufyan Salim Mahmood Al Dabbagh</li> <li>- Iqram Mohammed Hayek</li> <li>- Kusai Abu Hilal</li> </ul>	
<b>Chapter Fifteen Digital Signature Algorithm</b>	<b>113-115</b>
<ul style="list-style-type: none"> <li>- Sufyan Salim Mahmood Al Dabbagh</li> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Iqram Mohammed Hayek</li> <li>- Kusai Abu Hilal</li> </ul>	
<b>Part V Zero-Knowledge Proof</b>	<b>116</b>
<b>Chapter Sixteen Background of Zero-Knowledge Proof</b>	<b>117-120</b>
<ul style="list-style-type: none"> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Rusydi Hasan</li> <li>- Siti Khairunnisa Mohd Bakri</li> <li>- Nur Dalilah Bt More Yusoff</li> <li>- Nur Khairunnisa Bt Juara</li> </ul>	
<b>Chapter Seventeen Interactive Proof Systems</b>	<b>121-126</b>
<ul style="list-style-type: none"> <li>- Rusydi Hasan</li> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Siti Khairunnisa Mohd Bakri</li> <li>- Nur Dalilah Bt More Yusoff</li> <li>- Nur Khairunnisa Bt Juara</li> </ul>	
<b>Chapter Eighteen Zero-Knowledge Proof</b>	<b>127-132</b>
<ul style="list-style-type: none"> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Rusydi Hasan</li> </ul>	

- Siti Khairunnisa Mohd Bakri	
- Nur Dalilah Bt More Yusoff	
- Nur Khairunnisa Bt Juara	
<b>Chapter Nineteen Feige-Fiat-Shamir Identification Scheme</b>	<b>133-138</b>
- Rusydi Hasan	
- Imad Fakhri Taha Al Shaikhli	
- Siti Khairunnisa Mohd Bakri	
- Nur Dalilah Bt More Yusoff	
- Nur Khairunnisa Bt Juara	
<b>Part VI Secret Sharing</b>	<b>139</b>
<b>Chapter Twenty Introduction</b>	<b>141-146</b>
- Muhammad Israfil	
- Imad Fakhri Taha Al Shaikhli	
- Sufyan Salim Mahmood Al Dabbagh	
<b>Chapter Twenty One Shamir's Threshold Scheme</b>	<b>147-150</b>
- Imad Fakhri Taha Al Shaikhli	
- Sufyan Salim Mahmood Al Dabbagh	
- Muhammad Israfil	
<b>Chapter Twenty Two Blakely's Secret Sharing Scheme</b>	<b>151-155</b>
- Sufyan Salim Mahmood Al Dabbagh	
- Imad Fakhri Taha Al Shaikhli	
- Muhammad Israfil	
<b>Part VII Quantum Cryptography</b>	<b>156</b>
<b>Chapter Twenty Three Quantum Cryptography</b>	
- Azeddine Messikh	



## **7. Advanced Encryption Standard (AES)**

- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Muhammad Fadil Lubis
- Usman bin Mohd Azhar
- Nopan Ziro Ando

### **ABSTRACT**

In this article we will talk about the background of Advanced Encryption Standard (AES), description of AES and how we will encrypt the plaintext and decrypt the cipher text using that cipher. Also we will introduce into algorithm of AES and the cryptanalysis of AES.

### **DESCRIPTION OF AES**

In January 1997, the National Institute of Standards and Technology (NIST) started an open selection process for a new encryption standard. The NIST encouraged parties worldwide to submit proposals for the new standard. The proposals were required to support a block size of at least 128 bits, and three key sizes of 128, 192 and 256 bits. The selection process was divided into two rounds. In the first round, 15 of the submitted 21 proposals were accepted as AES candidates. The candidates were evaluated by a public discussion. The international cryptographic community was asked for comments on the proposed block ciphers. Five candidates were chosen for the second round: MARS (IBM), RC6 (RSA), Rijndael (Daemen and Rijmen), Serpent (Anderson, Biham and Knudsen) and Twofish (Counterpane). Three